E-CLIC European Collaborative Innovation Centres for Broadband Media Service	KARLSTADS UNIVERSITET

User friendly e-privacy

Exploring touch-screen biometrics
Case Study report

EUROPEAN UNION
European Regional Development Fund

Investing in the future by working together for a sustainable and competitive region

The Interreg IVB North Sea Region Programme

Executive summary

The use of mobile smart devices for storing sensitive information and accessing online services is increasing. At the same time, methods for authenticating users into their mobile devices and mobile online services that are not only secure, but also privacy and user-friendly are needed.

In this report we present the results of our explorations of the biometrics that can enhance the security of smart phones with touch-screens. This project was conducted in cooperation with the companies Gemalto in Gothenburg and Nordea in Copenhagen to explore means of secure authentications to mobile phones providing a “Trusted User Interface” (as developed by Gemalto). To address this challenge we developed an application for the Android mobile platform to collect data on the way individuals draw lock patterns on a touchscreen.

Using a Random Forest machine learning algorithm this method achieves an average Equal Error Rate (EER) of approximately 13.84%, meaning that lock patterns biometrics can be used for identifying users towards their device, but could also pose a threat to privacy if the users' biometric information is handled outside their control.

1 Introduction

Mobile devices have become an essential part of our daily lives and are used today for many sensitive applications including eBanking and eCommerce applications. However, despite all the information contained in a device and the transactions that can be performed with it, many users still choose not to protect their devices.

Currently, most of the solutions for authenticating users into their devices and other mobile services are based on the same solutions offered when using desktop computers, which usually involve the use of a PIN, a strong password, or some sort of extra external security token device. These techniques become cumbersome when applied to mobile devices and do not always provide a satisfactory user experience.

As a proposed solution to these issues we investigated how screen *lock patterns* can be enhanced with the use of biometric features. By lock patterns we refer to the option contained in the Android mobile platform for locking the phone's screen (Figure 1).

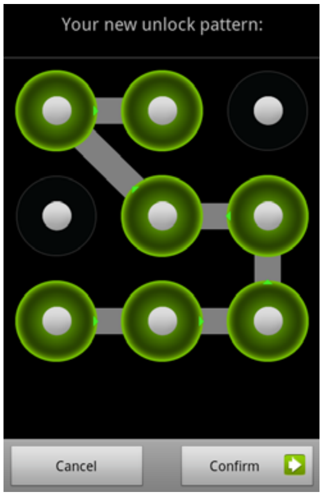


Figure 1. Android lock patterns

We hypothesized that adding biometric analysis to lock patterns can enhance the security of this type of graphical passwords by providing a two-factor authentication mechanism, and that it would be a privacy-friendly solution if it is used to protect the user’s information stored on the device.

Secure authentication methods are of key importance for mobile eBanking and eCommerce applications, for which users need to store securely encryption keys and credentials on their smart devices. Our industrial partner Gemalto is currently developing secure mobile device with a “Trusted User Interface” providing a secure path for data input by users, which can also establish a securely authenticated and encrypted connection to other banking or eCommerce servers. Using touch screen biometrics in combination with graphical passwords and the mobile phone providing a trusted user interfaces/trusted element, will provide a 3-factor authentication mechanism (by authenticating the user by what he knows (PIN), what he is (biometrics) and what he possesses (trusted phone), and thus increased security.

2 Related work

Research on biometrics using smart mobile devices has been conducted in the way people type keys on the on-screen keyboard or numeric pad. Also, on the unique ways people move when they walk or when they answer or place a phone call, by measuring the gyro sensors on the devices.

Researchers have also suggested the use of graphical passwords as an easier alternative to written passwords, based on the idea that people have a better ability to recall images than texts. Different usability studies have outlined the advantages of graphical passwords, such as their reasonable login and creation times, acceptable error rates, good general perception and reduced interference compared to text passwords, but also their vulnerabilities.

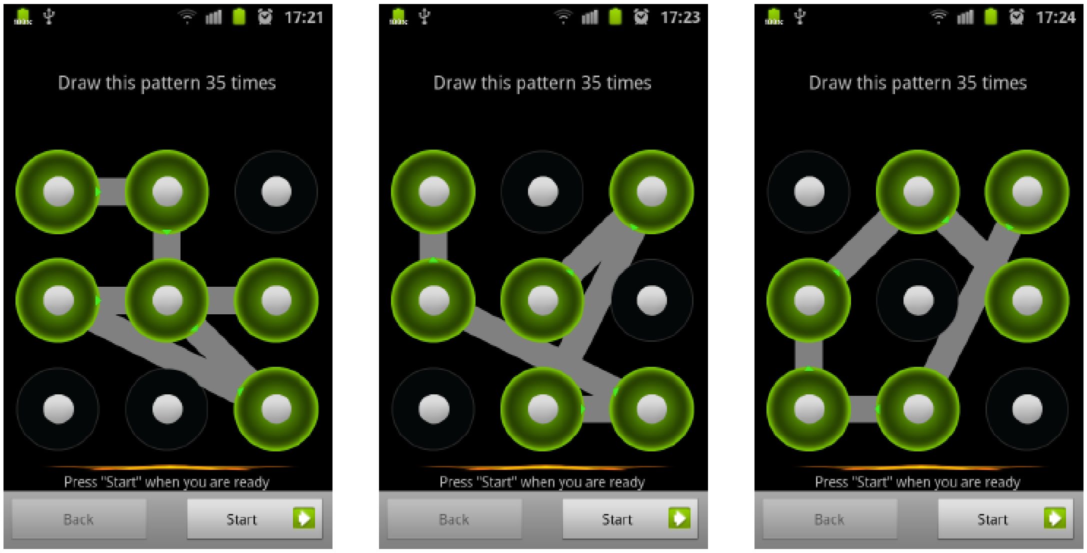
Regarding issues to users' anonymity, a recent study has demonstrated that pseudonyms chosen by users at different websites can be linked to deduce their real identity. Yet another study has shown that users' identities can be reconstructed from their typing patterns while browsing online. In our studies, we consider if similar privacy related issues could arise when employing the biometrics of lock patterns for authentication.

3 Experimental setup

We constructed a set of experiments to answer two main research questions:

1. **Do lock patterns provide a set of distinguishing features that are unique to each individual?** Is it possible to verify the identity of individuals by the way they draw a pattern on the screen?
2. **What are the privacy challenges that need to be considered when using this authentication method?** If users can be uniquely identified by the biometrics of lock patterns, what are the privacy issues to be tackled before this method can be used in practice?

Using Google's platform for mobile devices, Android, we developed a mobile application that collected data from different individuals on the way they move their finger across the screen with the purpose of unlocking their phone. Our data collection method consisted in asking 32 test participants draw three different lock patterns 50 times each, giving us a total of 150 trials per participant. The three patterns they were asked to draw can be seen in Figure 2.



Draw this pattern 35 times

Press "Start" when you are ready

Draw this pattern 35 times

Press "Start" when you are ready

Draw this pattern 35 times

Press "Start" when you are ready

Figure 2. The three different patterns that test participants were asked to draw 50 times each.

While the participants drew a pattern, two main features were captured for each successful trial: the finger-in-dot time, which is the time in milliseconds from the moment the participant's finger touches a dot to the moment the finger is dragged outside the dot area, and the finger-in-between-dots time, representing the speed at which the finger moves from one dot to the next. All erroneous trials were disregarded.

3.1 Data analysis

The data collected on the participants' finger movement times were used to calculate the common standard metrics used to assess biometric systems, the *False Acceptance Rate* (FAR) which indicates the probability that the system will erroneously grant access to an intruder, and the *False Rejection Rate* (FRR) which is the probability that the system will wrongly deny access to a legitimate user. The point at which both FAR and FFR are equal is denoted the *Equal Error Rate* (EER). The EER makes it easier to compare the performance of various biometric systems or classifiers, and the lower its value the better the classifier. The Random Forest classifier, for instance, has been previously used to analyze the keystroke dynamics of users entering PIN codes on computer keyboards. Using this classifier we obtained an EER of 13.84% when all the three patterns were combined.

Then, using statistical software we calculated a so called ROC curve (Receiver Operating Characteristic curve). This curve allows the evaluation of different machine learning algorithms by measuring the rate of false positives and true positives against a varying threshold level. The ROC curve in this case provided us with the formula $y = x^{(0.072 \pm 0.002)}$, from where we can infer that having a FAR of 10% would give us a probability of correctly admitting a legitimate user (a True Acceptance Rate or *TAR*) between 84.33% and 85.11% ($y = 0.10^{(0.072 \pm 0.002)}$). Therefore the value for FRR (*FRR* = 100% - *TAR*) lies between 14.89% and 15.67%.

4 Implications

Our results show that the security of mobile devices can be improved by enhancing a lock pattern mechanism with biometric features.

We consider this result to be a good beginning on the exploration of touch-screen dynamics given that the moderately low EER (13.84%) was obtained without applying any other analytical enhancements to the data (such as handling outliers, differentiating distances between dots, optimizing the human learning effect, grouping data by device, etc.).

Supposing that the pattern is only known to the legitimate user, the chances for an imposter to successfully authenticate into the system are further reduced. For example, given that there are 16,032 combinations of six-dotted patterns in the current implementation of the Android lock patterns, let the probability of an imposter entering the correct lock pattern on the first attempt to be Pr(*PatternGuessing*) = 1/16,032 = 0.00006. Adding biometrics to lock patterns, this probability is further reduced to 0.000006 (or 0.0006%), which makes it more secure than using 4- and 5-digit PINs (since they have a probability of 0.01% and 0.001% correspondingly).

Having this level of security improves also the privacy of the personal information stored inside the mobile device. However, we realized that some privacy concerns could also arise from the fact that people can be identified from the way they draw their finger on the screen. For example, third party phone apps, and even normal websites, could be recording the users’ finger movements on the background in order to identify users without their knowledge or consent.

Our results and its implications have been presented at the IFIP Summer School 2011, which dealt with various privacy issues on the digital age.

5 Conclusions and future work

The work presented here is our initial step towards finding user-friendlier methods for authentication into mobile smart devices. Our results show that adding biometric information to lock patterns can enhance the security of this method by providing two-factor authentication towards the smart device. A relatively low EER of 13.84% was achieved by analyzing the data from 32 individuals using a Random Forest classifier when combining the three different lock patterns and without any analytical enhancements to the data. This implies that users could be identified at this rate regardless of the pattern they draw.

Our plans for future work include the application of other machine learning classifiers and analytical enhancements to get a better EER. Also, we would like to expand this study to include the combination of different biometric methods (multimodal biometrics) and other secure technologies that can provide users with a seamless authentication experience into mobile applications that handle sensitive data.

Acknowledgments

This work is partly funded by the E-Clic project and the Swedish Knowledge Foundation (KK-stiftelsen) as part of the U-PrIM research project[1]. We thank our industrial partners Peter Gullberg from Gemalto and Loba van Heugten and Ernst Joranger from Nordea.

[1] U-PrIM – (Usable Privacy-enhancing Identity Management for smart applications) http://www.kau.se/en/computer-science/research/research-projects/u-prim